ISMS and ISO 27001: which certificate do you need, and will the system run your security?

Decide this quarter which evidence your customers and regulators actually ask for, such as an ISO/IEC 27001:2022 certificate or a TISAX label, because NIS2 and the German BSIG require documented measures, not a certificate[1]. Then scope the ISMS to all the regulated entity's relevant operations, let your risk register choose the controls and have management decide on the remaining risks at least once a year.

Reviewed **5 Nov 2026** | Next review **5 Dec 2026** | Version **1.1**

Written for **Security, compliance and IT leads in EU organizations, especially in Germany, deciding whether and how to build an ISMS**

Latest version **sheets.einblick.dev/isms/**

If you only do five things

1. **List who asks for which evidence.** Write down what key customers, regulators and insurers require. The BSI calls an ISO 27001 certificate a good foundation for the BSIG but no proof of NIS2 compliance[1].
2. **Scope the whole regulated entity.** ISO 27001 lets you limit the scope; the BSIG requires measures for all relevant operations of the entity[1]. Include IT operations, cloud services and outsourced process steps.
3. **Let risks choose the controls.** Derive controls from risk treatment, then check them against Annex A so none is left out by accident[8]. Under the BSIG, you can't just accept or transfer a relevant risk[1].
4. **Make management own the remaining risks.** ISMS responsibility can't be delegated, and management signs off residual risks[4]. Give every accepted risk an owner and an end date.
5. **Audit whether controls work.** Give internal auditors time to test the controls for your biggest risks[4]: restore a backup, sample leavers' accounts, trigger an alert.

Choose what to certify against

1. **Does a regulator name a scheme?** German power and gas grid operators need an ISMS certified against the Bundesnetzagentur's 2015 IT security catalog, now under revision; an ISO or IT-Grundschutz certificate alone isn't enough[16]. Other KRITIS operators prove their measures to the BSI every 3 years[3].
2. **Do automotive customers ask for TISAX?** More than ten vehicle makers and thousands of suppliers use TISAX results to judge partners[12]. Register the sites and objectives your customer names.
3. **Do customers or tenders ask for ISO 27001?** Get an accredited ISO/IEC 27001:2022 certificate, which can be recognized worldwide[8].
4. **Do you want the BSI's catalog behind it?** ISO 27001 on the basis of IT-Grundschutz needs a BSI-certified lead auditor; the BSI checks the report and issues the certificate[7].
5. **Does nobody ask for a certificate?** Build to ISO 27001 anyway and certify when asked. NIST CSF 2.0 helps report outcomes to the board, but NIST offers no certification[15].

The certifiable options side by side

ENISA maps each requirement of NIS2 Implementing Regulation 2024/2690 to ISO 27001 and NIST CSF 2.0, without judging equivalence or full coverage[11].

ISO/IEC 27001:2022

- **Current edition.** The 2022 text with Amendment 1:2024[9], which asks you to decide whether climate change is relevant; no new certificate is needed[10].
- **Controls.** Annex A refers to the 93 controls of ISO/IEC 27002:2022[8]. You select them by risk and list them in the statement of applicability (SoA).
- **2013 is gone.** Certificates to the 2013 edition expired or were withdrawn by 31 October 2025[8].

IT-Grundschutz and Grundschutz++

- **Classic.** Audited against BSI-Standard 200-2 and the Kompendium Edition 2023[6], for 3 years with yearly surveillance[7]. Certifiable until 30 November 2031[5].
- **Grundschutz++.** BSI-Standard 300-1 sets the method and a machine-readable catalog replaces the Kompendium. Certification applications open on 1 January 2027[5].
- **Less risk work.** For normal protection needs the BSI did the risk analysis; you cover high needs and gaps[4].

TISAX

- **Objectives set the depth.** AL2 checks evidence and interviews the security lead, usually by video call. AL3, for example for strictly confidential data and prototype parts, checks everything, generally on site[14].
- **Catalog.** VDA ISA2027 applies to assessments ordered from 1 January 2027[12]; initial ISA6 assessments can be opened until March 2027[13].
- **Validity.** Labels last up to 3 years[12].

What NIS2 and the BSIG require

- **No certificate.** The BSI says ISO 27001 certification is no precondition for meeting the BSIG[1], and IT-Grundschutz isn't mandatory for all entities[2].
- **Documented measures.** You must document how you meet the risk management duties[3] and show proof when the BSI orders it, for example audit reports. KRITIS operators submit it unasked[2].
- **Gaps to close.** Registration, reporting deadlines and management training aren't part of ISO 27001[1]; see the EU security laws sheet. Energy and telecom operators follow their sector law instead[3].

Scope and SoA, done honestly

- **Scope by business process.** Name the processes, sites, applications, IT systems and service providers, and include each process completely[4].
- **Mark each control's real state.** Implemented with evidence, planned with a date, or not applicable. Grundschutz++ allows that only if a requirement can't functionally be met or the component is absent, with a reason[4].
- **Explain every choice.** ISA2027 requires each listed aspect to be consciously considered and the decision explainable[12]. Hold your SoA to that.

- **Mappings are gap lists.** The BSI maps each § 30 BSIG measure to ISO 27001 clauses and controls[1]. ENX, which runs TISAX, argues that a label covering all affected sites meets NIS2 apart from reporting[14]; the BSI says no company certificate alone meets every BSIG requirement[2].

Run a risk assessment that changes decisions

- **Management sets the limits.** It approves the method, acceptance criteria and risk appetite[4]. Write criteria in euros, days of downtime and records exposed.
- **Start with the crown jewels.** Rate each business process for confidentiality, integrity and availability; Grundschutz++ advises starting with the most important one in the highest category[4].
- **Process owners own risks.** That is the default unless you decide otherwise[4]. Link each risk to measures with an owner and a due date.
- **Sign off and repeat.** Risk owners approve the plan and management the residual risks. Review at least yearly and after significant changes[4] or serious incidents.

- **Keep the documents few.** Scope, policy, objectives, risk register, SoA, treatment plan, audit and corrective action records and review minutes. Management approves the policy; every employee gets it[4].

Audits and reviews that change things

- **Aim audits at your risks.** Plan the program around the top risks, detection and incident handling, and earlier findings[4]. Test real samples.
- **Look for improvements.** Grundschutz++ sees internal audit as a way to find improvements, not just nonconformities[4].
- **Keep it impartial.** Pick an objective audit team and keep the security officer role apart from IT management[4].
- **End the review with decisions.** Cover audit results, performance, incidents, risk treatment, threat changes and earlier decisions[4]. Record decisions on budget, scope and accepted risks.

What changed in 2026

- **Grundschutz++ arrived.** BSI-Standard 300-1 version 1.0, dated 20 October 2026, targets experienced early adopters[4]. Certification applications on its basis open on 1 January 2027; classic IT-Grundschutz stays certifiable until 30 November 2031[5].

- **TISAX moved to yearly catalogs.** Under ISA2027, published on 1 July 2026, suppliers to organizations with very high protection needs are expected to show a TISAX label, an equivalent assessment or a supplier audit. New catalogs follow each summer[12].

What you can skip

- **A policy for every Annex A control.** Write rules where people need them; for technical controls, configuration exports are better evidence.
- **A GRC tool before the first cycle.** A spreadsheet register and your ticket system will do.
- **Separate programs for ISO, TISAX and NIS2.** Keep one register and one SoA with a column for each mapping.
- **Waiting for Grundschutz++.** Its method requirements mirror ISO 27001 clauses 4 to 10[4], so scope, risk and audit work carries over.
- **A climate change study.** Record whether it is relevant and why; IAF treated the amendment as a clarification[10].

Mistakes that cost the most

- **A scope too narrow to matter.** A certificate for the IT department alone misses what customers and the BSI care about. The BSI tells certified entities to check whether NIS2 needs a wider scope[1].
- **Controls copied from a template.** An SoA with every control implemented and no evidence falls apart in the first customer audit.
- **An ISMS run only by consultants.** Management can't hand over responsibility, and a security role must be involved in security-relevant projects such as new systems[4]. Let consultants coach the process owners.
- **Trusting a supplier's logo.** Ask for the certificate's scope and SoA; see the third-party risk sheet.

What this looks like at your size

Small team, no security staff

- Build to ISO 27001 without certifying until a customer asks.
- Name a security officer with budgeted time and a deputy.
- Hold the risk review and management review in one half-day meeting a year.

Growing, with IT or security staff

- Certify where customers ask, then widen the scope to the whole regulated entity.
- Check your SoA against the BSI's § 30 BSIG mapping[1] and, for digital providers, ENISA's table[11].
- Test one top-risk control each quarter.

Enterprise or regulated

- Align certification audits with the 3-yearly KRITIS proof to the BSI[3].
- With many sites and a central ISMS, ask about a TISAX simplified group assessment[14].
- Report effectiveness measures to the board quarterly.

Version history

5 Nov 2026, version 1.1	Moved the IAF document links to Global Accreditation Cooperation, which replaced IAF and ILAC on 1 January 2026, and stated the end of classic IT-Grundschutz certification as the BSI words it.

Sources

1. #nis2know: ISO/IEC 27001. BSI, checked 5 Nov 2026. bsi.bund.de
2. Fragen und Antworten zu NIS-2. BSI, checked 5 Nov 2026. bsi.bund.de
3. BSIG §§ 28, 30 and 39. BMJV, checked 5 Nov 2026. gesetze-im-internet.de
4. BSI-Standard 300-1, v1.0. BSI, 20 Oct 2026. bsi.bund.de
5. Grundschutz++ Meilensteinplan. BSI, Oct 2026. bsi.bund.de
6. IT-Grundschutz Prüfgrundlage, v4.8. BSI, 1 Feb 2026. bsi.bund.de
7. IT-Grundschutz Zertifizierungsschema, v2.2. BSI, 1 Feb 2026. bsi.bund.de
8. IAF MD 26:2023. IAF (now Global ACI), 15 Feb 2023. sys.global-aci.org
9. ISO/IEC 27001:2022, Amd 1. ISO, checked 5 Nov 2026. committee.iso.org
10. Climate communiqué. IAF (now Global ACI), 22 Feb 2024. global-aci.org
11. NIS2 guidance mapping table, v1.2. ENISA, 21 Aug 2025. enisa.europa.eu
12. VDA ISA2027 released. ENX, 1 Jul 2026. enx.com
13. TISAX downloads. ENX, checked 5 Nov 2026. enx.com
14. NIS2 fulfilment through TISAX, v1. ENX, 24 Apr 2025. enx.com
15. CSF FAQs. NIST, checked 5 Nov 2026. nist.gov
16. IT-Sicherheitskatalog. BNetzA, checked 5 Nov 2026. bundesnetzagentur.de